Disaster Recovery/Business Resumption Planning

in Washington State Government

July 1992

Prepared by:
Washington State
Department of Information Services
George Lindamood, Director
PO Box 42440
Olympia, WA 98504-2440

Adopted by:
Washington State
Information Services Board
Len McComb, Chair

Disaster Recovery/Business Resumption Planning
TABLE OF CONTENTS

Plan

Summary

Establishes statewide policy for disaster recovery/business resumption planning. Includes standards that will serve as the basis for compliance monitoring. Addresses risk analysis, business impact analysis, agency policies, and procedures for recovering from a variety of service interruptions -- short outages to destruction of data centers.

Background

An agency disaster recovery plan is currently included as a section of the agency Data Processing Security Plan.

Some agencies, e.g., Department of Transportation, have conducted extensive planning and have contracted for backup recovery services for their mainframe computers.

A perusal of data processing security plans filed with the Policy and Regulation Division (PRD) indicates only limited planning for disaster recovery on the part of most agencies.

Agencies that use the Department of Information Services (DIS) as their principal provider of mainframe services tend to assume DIS would effect recovery of their systems when necessary.

Agencies tend to focus concern on mainframe computers and minicomputers and pay only cursory attention to the recovery of microcomputers, voice, and data telecommunications services.

DIS completed its disaster recovery plan for the two data centers in 1991. This culminated an effort which began in July 1989 and has resulted in successful testing of both the 370 platform and the UNISYS platform backup recovery capabilities at their respective recovery facilities. The contractor, Deloitte & Touche, found deficiencies in a number of areas, including policy, during the course of this project.

Deloitte & Touche made several recommendations urging a substantial change from past practice; one called for segregating the state's Automated Data Processing (ADP) Security Policy into two distinct sections: (1) Data Security and (2) Disaster Recovery Planning. The latter policy " . . . should not only cover disaster recovery for the computer and its processing environment but also the entire telecommunications network from the customer terminal through the front-end processor at the data center."

Deloitte & Touche also recommended ". . . auditing disaster recovery plans on a regular basis to ensure they have been tested and reflect the current business practices, priorities, and needs of the customer agency."

The Dolan Report based its opinions regarding disaster recovery planning on the published findings and recommendations from the Deloitte & Touche project.

PRD elected to segregate disaster recovery planning from information security and develop separate policies. The policy presented herein is a response to recommendations from consultants.

Agency impact

The policy will assist agencies to:

1. Identify information technology (IT) resources that are at risk.
2. Implement useful plans to protect against identified threats and mitigate risk.
3. Implement tested emergency procedures when a disaster occurs.
4. Implement and test procedures that enable short-term recovery of IT services following a disaster.
5. Develop, by 1993, a plan that will enable full recovery and the resumption of normal operations.

Impact on agency resources:

1. Agencies will have to expend time, energy, and budget on the effort required by this policy.

Policy

Purpose

It is the intent of the Information Services Board (ISB) that state agencies will:

1. Develop, implement, maintain, and test disaster recovery plans.
2. Train their employees to execute the recovery plans.
3. Take the steps needed to mitigate the impact of disasters.

Each agency must be able to demonstrate the ability to continue to provide mission-critical, IT-dependent services during recovery from a serious, business interruption or disaster.

For purposes of this policy, "disaster recovery/business resumption planning" includes, but is not limited to, the documentation, plans, policies, and procedures that are required to restore normal operation to a state agency impacted by manmade or natural disaster.

The three principal priorities of disaster recovery/business resumption planning are:

1. To save data.
2. To save hardware, software, and facilities.
3. To resume critical processes and restore data.

Scope

This policy applies to all state agencies that operate, manage, or use information technology (IT) services to support critical business functions. The policy does not address the resumption of business functions other than those dependent upon IT services. The policy assumes agencies have in place, or will develop, plans for full, business resumption.

The scope includes, but is not limited to:

1. Agencies that operate, manage, or use stand-alone, shared, or network-attached computers, whether mainframes, mid-range, or microcomputers for their own use or for use by other agencies.

2. Agencies that operate, manage, or use voice, data, or video telecommunications equipment, networks, or services for their own use or for use by other agencies.

3. Agencies that purchase computer services or telecommunications netwo rk services from other state agencies or commercial concerns.

Policy Statements

Agencies shall develop disaster recovery/business resumption plans.

Agencies dependent on voice telecommunications, data telecommunications, video telecommunications, or computer services for carrying out their missions must develop disaster recovery/business resumption plans. Each agency is responsible and accountable for its own disaster recovery/business resumption program. Agencies that purchase computer services or telecommunications services from other state agencies or commercial concerns shall integrate their disaster recovery/business resumption plans, including off-site storage of data, with service providers.

Agencies shall document disaster recovery/business resumption plans.

Agencies shall document disaster recovery/business resumption plans in accordance with the standards provided by this policy.

Agencies shall maintain disaster recovery/business resumption plans.

Agencies shall update disaster recovery/business resumption plans at least annually and following any significant change to their computing or telecommunications environment. Agency directors shall review and approve their agency's updated plan.

Agencies shall test disaster recovery/business resumption plans.

Agencies are required to test their plan at least once a year.

The type and extent of testing adopted by an agency will depend on:

1. Criticality of agency business functions.
2. Cost of executing the test plan.
3. Budget availability.
4. Complexity of information system and components.

Agencies shall prepare a report documenting their test plans and the results achieved. Agencies shall correct any deficiencies revealed by the test. Agency directors shall review and approve the test plan and test report.

Agencies shall train employees to execute disaster recovery/business resumption plans.

Training will consist of:

1. Making employees aware of need for a disaster recovery/business resumption plan.
2. Informing all employees of the existence of the plan, and providing procedures to follow in the event of an emergency.
3. Training recovery team members to perform the disaster recovery/business resumption procedures.
4. Providing the opportunity for recovery teams to practice disaster recovery/business resumption skills.

Agencies shall file plans with DIS.

Each agency required to file an IT plan shall file a copy of its business resumption plan with DIS/PRD not later than July 1 of each odd-numbered year.

DIS shall assist with review and serve as focal point for disaster recovery/business resumption planning.

DIS/PRD shall:

1. Assist agencies with disaster recovery/business resumption planning for IT.
2. Review completed agency disaster recovery/business plans.
3. Serve as IT focal point for statewide disaster recovery/business recovery planning.

The State Auditor may audit disaster recovery/business resumption plans.

The State Auditor may audit agency disaster recovery/business resumption plans and tests for compliance with standards.

Effective Date

Agencies must comply with this policy and related standards by July 1, 1993.

Exception:
Agencies that cannot meet the due date for submittal of their disaster recovery/business resumption plan may request a deferment from the ISB. Such a request will set forth the rationale justifying an extension and commit to a date when the plan will be submitted. The ISB will review and either approve or disapprove the request.

Maintenance

Technological advances and changes in the business requirements of agencies will necessitate periodic revisions to this policy and its standards and guidelines. DIS/PRD is responsible for routine maintenance of the policy and its standards and guidelines to ensure timeliness and accuracy; only major policy shifts require ISB approval.

Statutory Authority

Revised Code of Washington (RCW), 43.105.041 (3) empowers the ISB:

"To develop statewide or interagency technical policies, standards, and procedures."

The RCW, 43.105.041 (7) empowers the Board:

"To establish policies for the periodic review by the department [DIS] of agency performance which may include but are not limited to analysis of: (a) Planning, management, control, and use of information services . . ."

Standard

Planning Standard

Agency disaster recovery/business resumption plans shall provide all applicable information required by this standard.

All state agencies and educational institutions using or providing computing or voice, data, or video telecommunications services must prepare Disaster Recovery/Business Resumption Plans.

Included are:

Agencies with their own computing or telecommunications facilities.

Agencies that provide computer or telecommunications services to others.

Agencies using computing or telecommunications services supplied by providers external to their organization.

Each agency is responsible and accountable for its own disaster recovery/business resumption program. Agencies using external services shall coordinate their disaster recovery/business resumption plans with service providers.

The disaster recovery/business resumption plan is primarily for agency use. Agencies may adapt this standard to meet individual needs, but all applicable elements of the standard must be included in their plan. A disaster recovery/business resumption plan must contain enough information to enable agency management to assure the agency's ability to resume mission-critical computing and telecommunications services and operations. A disaster recovery/business resumption plan may contain references to another organization's disaster recovery/business resumption plan, or to an agency's internal policy, standards, or procedures manual. The agency shall, upon request, make referenced material available for review or audit by DIS.

Agencies shall review, update, and test their disaster recovery/business resumption plans annually, or more frequently if appropriate. Agencies must update their plans whenever agency computing or telecommunications environments undergo significant changes. Such changes may include: physical facility, computer hardware/software, telecommunications hardware/software, telecommunications networks, application systems, organization, or budget.

If an agency purchases IT services from another organization, the agency must make certain its disaster recovery/business resumption plan for those services fits with the service provider's plan. If two or more agencies participate in operating an information service facility, they must develop a joint disaster recovery/business resumption plan which meets their mutual needs.

Contents

Overview

Describe the purpose and organization of the plan. Document state procedures for updating and distributing the plan. Describe the process for periodic (at least annual) testing of the plan.

Business Impact Analysis

Document the operational, legal, and financial impact from a disruption or disaster affecting any computer or telecommunication service area of the agency.

Risk, Threat, and Vulnerability Analysis

Document the threats that could debilitate computer or telecommunication service areas and cause business interruption; determine the probability of occurrence of each identified threat. Determine the vulnerabilities of service areas to potential threats. Estimate the loss potential of a service area, either by quantitative or qualitative means. Define the level or duration of service outage that constitutes a disaster or triggers the recovery plan.

Recovery Strategy

Document the general recovery strategy that the agency will use in event of a disaster. There are different levels or degrees of disaster. Procedures should aim at coping with the worst case. Start with a narrative of the agency's strategy for managing the disaster situation. The recovery strategy is an overview of the recovery process that the organization will follow if affected by a disaster. The strategy should address:

1. Recovery requirements for critical business operations.
2. A description of provisions for off-site storage of critical dat a.
3. A description of the agency's alternative processing strategies and facilities such as:

    a. Command centers.
    b. Alternate business operations.
    c. Alternate data processing.
    d. Alternate data communications.
    e. Alternate voice communications.

4. Procedures for obtaining resources during both the recovery phase and the restoration phase.

Emergency Response/Problem Escalation

Emergency response/problem escalation procedures prescribe how to respond to two kinds of situations:

1. **Disaster events**. Fires, floods, earthquakes, and bombings are examples of disaster events. They often take the form of unforeseen events that cause damage

or lengthy disruption or threaten to do so. One can often more readily recognize the situation is a disaster with these types of occurrences.

2. **Problems**. Disasters may evolve from problems that disrupt normal operations and then worsen or continue so long the disruption becomes critical. Examples: power "brownout," a computer virus, inclement weather, flu epidemic, sabotage, negligence, disk drive failure, local telephone service failure, or software failure.

Disaster recovery plans should address specific procedures for both situations. Emergency procedures direct the response to disaster events. Escalation procedures direct the response to problems. Both sets of procedures may result in the declaration of a disaster and activation of the recovery plan.

Emergency Response

Disaster recovery plans should document the emergency response actions the agency must take immediately to:

1. Protect the lives and safety of all personnel.
2. Gain immediate emergency help from fire, police, hospitals.
3. Reduce outage duration or loss of IT services or assets.
4. Inform staff who are members of the agency disaster recovery/business resumption management team a serious loss or interruption in service has occurred.
5. Set up a focal point for coordinating the recovery program, sending out information, and assembling personnel.
6. If appropriate, establish contact with the Office of Emergency Management.

Problem Escalation

Disaster recovery plans must state the steps to follow for escalating unresolved problems to disaster status. The purpose of problem escalation procedures is to define the steps and time intervals leading up to the declaration of a disaster.

These procedures require use of a "contact tree", a list of individuals to be notified of the situation at specified time durations following the onset. The contact tree represents an ever-widening circle of management and key technical people. Such a procedure ensures key decision makers become aware of the situation in order to make more timely and informed decisions. As the situation becomes more pressing, the procedure must trigger calls to the disaster recovery/business resumption team, upper levels of management, clients, suppliers, and the public.

Plan Activation

First alert procedures:

Document general guidelines for initial notification of a potential disaster situation.

Disaster confirmation procedures:

1. Document procedures to manage the initial assessment of a disaster or potential disaster situation.
2. Document the procedures and specify the personnel necessary to assess the damage and determine the level of severity of the incident.
3. Document procedures for reporting findings to management.
4. Document procedures for making initial emergency contacts.
5. Document procedures for possible command center activation.
6. Document recovery team notification procedures.
7. Document procedures for declaring a disaster. Describe the decision support mechanism required to declare a disaster--versus a less severe interruption in processing capability.
8. Document procedures for informing employees, the public, customers, and suppliers.

Recovery Operations

Recovery flow:

Outline or chart the sequence of steps to follow when a disaster situation has occurred or potentially may occur.

Recovery team organization:

1. Document staff and management responsibilities for putting the recovery plan into effect.
2. Identify an alternate for each team member.
3. Include team or individual assignments of responsibility by area of expertise such as:
    a. Technical staff in the areas of systems software, telecommunications, and computer operations.
    b. Program staff and management to aid in resolution of programmatic issues.

c. Business services to support such tasks as arranging for office space, supplies, equipment, and processing of emergency contracts.

4. Personnel and communications staff to issue information about special work assignments, conditions, or locations.

Recovery team plans:

1. Document the procedures required to achieve recovery rapidly. A portion of this documentation should consist of the process for recovering the critical data-processing activities. If appropriate, the latter should encompass transition to manual procedures and logistics of moving to an alternate facility.

2. Procedures for each team should, at a minimum, consist of:

   a. Team charter.

   b. Membership.

   c. Interfaces.

   d. Preparation requirements.

   e. Action procedures.

   f. Appendices.

Primary site restoration or relocation:

Document the procedures to use after the interim processing situation has stabilized. The intent is to provide a framework for restoring full processing capability at a permanent location.

Plan Validation/Testing

Document the disaster recovery/business resumption plan testing program. Specify necessary tests and assign responsibility for overseeing testing. Clearly state the purposes for conducting tests of the recovery plan. Include the policies and guidelines that will apply to testing of the

Training

Specify the aims, training activities, schedule, and an administrator for agency disaster recovery/business resumption training. Describe regularly occurring training activities.

Plan Maintenance

Assign plan maintenance responsibility. Provide a schedule for regular, systematic review of the content of the disaster recovery/business resumption plan. Document the procedure used for making changes to the plan. Provide policies and procedures for distributing the disaster recovery/business resumption plan and updates to the plan. The disaster recovery/business resumption plan may contain sensitive information about the agency's business, communications, and computing operations. Policy and procedures for distribution of the plan should take this into account.

Appendices

Agencies may attach a variety of appendices to the plan. The plan sections described above should contain static procedures. Appendices should contain information that needs continual updating.

Examples of content are:

1. Emergency action notification information containing the names and phone numbers of management, staff, recovery team members, vendors, suppliers, service providers, and customers.
2. Damage assessment or disaster classification forms intended to support the management decision process.
3. Profiles of critical applications.
4. Agency hardware, software, office space, and office furniture inventories.
5. Voice and data communications network routing information necessary to provide interim processing capability.

This page intentionally left blank.

Guidelines

Guidelines for Disaster Recovery/Business Resumption Planning

Emergency response/problem escalation procedures prescribe how to respond to two kinds of situation:

1. **Disaster events**. Fires, floods, earthquakes, and bombings are examples of disaster events. They often take the form of unforeseen events that cause damage or lengthy disruption or threaten to do so. One can more readily recognize the situation is a disaster during this type of occurrence.

2. **Problem**. A disaster may evolve from a problem that disrupts normal operations and then worsens or continues so long that disruption becomes critical.

Disaster recovery/business resumption plans should specify procedures for both situations. Emergency procedures direct the response to disaster events. Escalation procedures direct the response to problems. Both sets of procedures may result in the declaration of a disaster and activation of the recovery plan.

The purpose of disaster recovery/business resumption planning is to assure continuity of computing and telecommunications operations needed to support critical agency functions. The business resumption plan should aim at achieving a systematic and orderly resumption of all agency computing and telecommunications services. The plan should provide for restoring service as soon as possible. Those functions that are most critical to achieving the agency mission must remain in operation during the recovery period.

The Recovery Planning Process

There are nine major phases in the recovery planning process:

1. **Project Planning**: Define the project scope, organize the project, and identify the resources needed.

2. **Critical Business Requirements**: Identify the business functions most important to protect, and the means to protect them. Analyze risks, threats, and vulnerabilities.

3. **Recovery Strategies**: Arrange for alternate processing facilities to use during a disaster. Make sure to store copies of computer files, work-in-process, software, and documentation in a safe place.

4. **Emergency Response/Problem Escalation**: Specify exactly how to respond to emergencies and how to tell when a "problem" has become a potential "disaster."

5. **Plan Activation Procedures**: Determine procedures for informing the right people, assessing the impact on operations, and starting the recovery efforts.

6. **Recovery Operations**: Develop the specific steps for reducing the risks of an outage and restoring operations should an outage occur.

7. **Training**: Make sure everyone understands the recovery plan and can carry it out efficiently.

8. **Testing**: Make sure the plan works effectively.

9. **Maintenance**: Make changes and additions to keep the plan current.

The disaster recovery/business resumption planning process provides the preparation necessary to design and document the procedures needed to assure continued agency operations following a disaster. Each agency's process should include the following elements:

Project Planning

Get preliminary management commitment.

Get agreement from senior management on the need for disaster recovery/business resumption planning.

Designate a disaster recovery/business resumption manager.

Designate a person to manage the agency's recovery from a disaster. The designated individual must have sufficient knowledge of information management and information technology (IT) within the agency in order to work effectively with IT hardware and software, the data centers, and service providers in reestablishing information processing and telecommunications services after a disaster has occurred.

Organize a disaster recovery/business resumption planning team.

Organize a team that will be responsible for the detailed technical analysis and planning functions needed for a recovery plan.

Identify individuals from management, data processing, telecommunications, business operating units, and consultants to participate in preparing the disaster recovery/business resumption plan.

Audit current recovery preparedness.

Determine what security/disaster recovery/business resumption plans are in place. Identify what planning remains to be done.

Develop the project schedule.

Estimate task durations, identify responsibilities, assign resources, and document the schedule for plan development.

Specify documentation procedures.

Define recovery program overview.

Identify the scope and aim of the disaster recovery/business resumption plan.

Determine Requirements

An agency may carry out hundreds of operations that management and staff consider important. Key resources may be unavailable during a disaster. The agency must concentrate its resources on the operations that are most important for public health, safety and welfare. The aim of a disaster recovery/business resumption plan is to reduce potential losses, not to duplicate a business-as-usual environment.

1. Perform business impact analysis. Establish an understanding of the business organization and service areas of the agency.

2. Identify the business functions to be addressed in accomplishing a business impact analysis.

    a. Identify essential business functions. Essential business functions are those functions that must take place in order to support an acceptable level of business continuity for the agency.

    b. Develop an understanding of service areas and interdependencies of the essential functions identified.

    c. Establish the priorities of senior agency management. Establish the scope of each service area's disaster recovery/business resumption plan and disaster recovery assumptions. There are three major tasks in this procedure:

        (1) Identify key senior management personnel.
        (2) Schedule and conduct interviews.
        (3) Summarize continuity concerns and priorities.

    d. Document the operational and financial impact that could result from a disruption or disaster affecting a service area of the agency. There are four tasks in this procedure:

        (1) Gather operational and financial impact data.
        (2) Develop outage impact scenarios.
        (3) Analyze operational impact.
        (4) Analyze economic impact.

    e. Criteria for establishing the criticality of business functions:

        (1) The key principle involved is that only those functions that must be performed because they are key to the survival of the organization should be listed as a top priority. The priorities of an agency may change as the duration of the service interruption lengthens. For

example, a function that can sustain a delay of 3 days may become a top consideration if the interruption lasts a week.

(2) The following criteria are suggested for determining the criticality of business functions. There may be others that are of importance to an agency.

- Maintenance of public health and safety.
- Income maintenance for citizens.
- Income maintenance for government employees.
- Payments to vendors for goods and services.
- Requirements for compliance or regulation.
- Effect on state government cash flow.
- Criticality Classification.
- Effect on production and delivery of services.
- Volume of activity and recovery costs.
- Effect on public image.
- Inter-system dependency.

The following categorization is suggested as a means for classifying computer application systems used by an agency:

Category/Classification

1. Must be processed in normal mode; no degradation is acceptable.
2. Only high priority; e.g., high dollar item transactions or critical reports will be processed.
3. Processing will be carried out on a "time available" only basis.
4. Processing will be suspended, but data collection will continue .
5. No processing or data collection will be carried out until normal computer capacity is reestablished.
6. Perform threat, risk, and vulnerability analysis.

    a. Determine the threats that could debilitate service areas and cause business interruption.

    b. There are many natural and manmade threats to service areas which could cause business interruption. Potential threats to consider include personnel, physical environment, hardware/software systems, telecommunications, applications, and operations.

    c. Threats affecting contingency planning.

        (1) Natural hazards:

            - Earthquake
            - Tornado
            - Flooding
            - Tsunami
            - Landslide
            - Volcanic eruption
            - Lightning
            - Smoke, dirt, dust
            - Sandstorm or blowing dust
            - Windstorm
            - Snow/ice storm

        (2) Accidents:

            - Disclosure of confidential information
            - Electrical disturbance
            - Electrical interruption
            - Spill of toxic chemical

        (3) Environmental failure:

            - Water damage
            - Structural failure
            - Fire
            - Hardware failure
            - Liquid leakage

- Operator/user error
- Software error
- Telecommunications interruption

(4) Intentional acts:

- Alteration of data
- Alteration of software
- Computer virus
- Bomb threat
- Disclosure of confidential information
- Employee sabotage
- External sabotage
- Terrorist activity
- Fraud
- Riot/civil disturbance
- Strike
- Theft
- Unauthorized use
- Vandalism

d. Determine the probability of occurrence of an identified threat.

(1) Many potential threats occur regularly. For regularly occurring threats, historical occurrences and statistical probabilities are maintained by organizations such as the Federal Emergency Management Agency (FEMA), the Federal Communication Commission (FCC), and the US Fire Administration. Statistics on naturally occurring disasters, burglaries, power outages, fires, and storms are usually available from local, state, or federal agencies.

(2) Local threats to the service area, such as hardware failures and unauthorized data access attempts, are usually logged in the organization's problem tracking system or management status reports.

(3) Factors affecting threat occurrence rate:

- Location
- Facility environment
- Data sensitivity/criticality
- Protection and detection features
- Visibility
- Proficiency level
- Security awareness
- Emergency training
- Staff morale
- Local economic conditions
- Redundancies

- Availability and use of written operating and security procedures
- Compliance level (measure of the level of observance or enforcement of security procedures)
- Past prosecutions

e. Determine the vulnerabilities of service areas to potential threats.

(1) Vulnerability the state of being open to abuse or misuse, or subject to indiscriminate use. A weak point or soft spot, a likelihood for error.

(2) For many threats, the vulnerability to a business interruption can be mitigated with controls. For example, a vulnerability to fire damage can be mitigated with Halon fire extinguishers and smoke alarms, as well as preventive policies such as the banning of cigarette smoking near flammable materials. Vulnerability considerations include natural disasters, environment, facility housing, access, work scene, and data

(2) In the qualitative approach, the probability and impact of an event are estimated in orders-of-magnitude, qualitative terms such as low, medium or high.

Recovery Strategies

Off-site storage of back-up material.

1. Select off-site storage locations.

   a. Identify one or more locations off-site for secure storage of copies of data, documentation, and critical supplies.

   b. Agencies that purchase computer services from external providers should arrange with the service-provider for off-site storage.

2. Determine off-site storage inventory. Identify specific files, programs, documentation, vendor contracts, supplies, etc. copies of which should be stored and maintained off-site. Agencies shall include at least one current copy of their disaster recovery/business resumption plan in the off-site storage inventory.

3. Specify off-site inventory procedures. Determine procedures, schedules, and responsibility for maintaining the contents of the off-site storage facility.

4. Alternate processing capability.

   a. Identify requirements for recovery facilities.

   b. Determine hardware processing capacity, phone service, data communications service, furniture, and space needed in an alternate processing facility.

5. Select recovery facilities.

   a. Rank potential recovery alternatives and select one or more.

   b. Produce recovery site procedures guide(s).

   c. Document information needed to use at each recovery facility.

6. Document overall recovery strategy .

   a. Document the general strategy that the agency will use in the event of a disaster.

      (1) The recovery strategy is an overview of the recovery process that the organization will follow if hit by a disaster. The strategy should address:

- Recovery requirements for restoration of critical business operations.
- Any alternate processing facilities employed.
- Any alternate manual procedures, forms, staffing, and space.
- Procedures for obtaining resources.

b. Agencies should also develop strategies for ad dressing each of the following where relevant:

(1) Command centers
(2) Alternate business operations
(3) Alternate data processing
(4) Alternate data communications
(5) Alternate voice communications

c. Recovery resource acquisition.

Emergency Response/Problem Escalation

Identify potential threats and develop emergency procedures.

Document the action steps to be taken immediately in responding to damaging events or threats of damage or disruption. Inform all agency staff of documented action steps.

1. The purpose of emergency procedures is to:

   a. Protect people.
   b. Protect property.
   c. Reduce outage duration or loss of IT services or assets.

2. Document the emergency response actions the agency must take immediately to:

   a. Protect the lives and safety of all personnel.
   b. Gain immediate emergency help from fire, police, hospitals.
   c. Reduce outage duration or loss of IT services or assets.
   d. Inform agency staff who are members of a Disaster Recovery/Business Resumption Management Team that a serious loss or interruption in service has occurred.
   e. Set up a focal point for coordinating the recovery program, sending out information, and assembling personnel.

3. Specify problem escalation guidelines.

   a. State the steps to follow for escalating unresolved problems to disaster status.
   b. The purpose of problem escalation procedures is to define the steps and time allotments leading up to the declaration of a disaster.

Plan Activation

Develop first alert procedures.

1. Prepare general guidelines for initial notification of a potential disaster situation.

2. Develop disaster confirmation procedures.

    a. Develop procedures to manage the initial assessment of a disaster or potential disaster situation.

        (1) Develop procedures for reporting findings to management.
        (2) Develop procedures for making initial emergency contacts.
        (3) Develop procedures for possible command center activation.

    b. Develop damage assessment procedures.

        (1) Develop procedures for damage assessment.
        (2) Develop procedures for examining the effect of the damage on processing of critical operations.

3. Develop notification procedures.

4. Develop procedures for declaring a disaster, for setting up a command center, and for informing the recovery teams, customers, the public, and suppliers.

Recovery Operations

- Determine plan activation flow.

- Outline or chart the steps to follow when a disaster situation has occurred or potentially may occur.

- Define recovery team organization.

- Determine the teams that make up the recovery organization.

- Develop team action plans. There may be several recovery teams, each specializing in some area of technical expertise. Disaster Recovery/Business Resumption Team procedures for each team should use a format like the following:

Team Charter or Function: The particular duties and responsibilities of this team in the event of a disaster.

Team Membership and Organization: The structure of the team, job titles of team members, reporting responsibilities.

Team Interfaces: Include detailed explanations of all the actions to be taken by this team prior to a disaster situation so it can function effectively, with the necessary data, personnel and other resources, if a disaster occurs. This section should cover relationships with vendors, customers, ongoing tasks to ensure readiness of the plan, training requirements, identification of critical resources, data, and personnel.

Action Procedures: This section provides an outline of the tasks to be carried out. It is written with the assumption that the team members know how to do their jobs and just need a guide to ensure that nothing is omitted during the normal confusion that will occur in the situation.

Procedures should be designed to be flexible in order to permit their use in varying types and degrees of contingency situation.

Procedures should be detailed enough to permit dependency upon them when no other documentation or knowledge is available.

Appendices: The appendices should contain the material and data that will be used in the event of an actual disaster. Include separate appendices on notification of personnel, resource requirements, forms and documentation, and any other subjects that are required. The requirement is based upon the ability of the particular team to access the information during a disaster. If the data may not be otherwise available, it should be included in the appendix to the disaster recovery/business resumption plan.

Training

Design a disaster recovery/business resumption training program.

1. Specify the aim, training activities, schedule, and an administrator for disaster recovery/business resumption training.

2. Develop specific training activities.

3. Develop an instructional plan for each training activity.

4. Develop training evaluation tools.

5. Develop techniques aimed at answering the following questions:

    a. Are trainees able to perform their recovery responsibilities?
    b. How can the agency improve training?
    c. How can the agency improve its disaster recovery/business resumption plan?

Testing

Testing is the only method to ensure that:

1. Recovery procedures are complete and workable.

2. Materials and computer files are available and can be used for alternate processing of critical operations and applications.

3. Backup copies of software, documentation, and work-in-process records are adequate and current.

4. Training of personnel was effective.

Design a recovery plan testing program.

1. **Detail**. Specify tests and assign responsibility for overseeing testing. Agencies using external services shall plan, schedule, and conduct their disaster recovery/business resumption plan testing in cooperation with service providers. The cost of establishing the necessary communication link and running a test at a remote back-up facility is high. A full test involving all agency applications may well be impractical due to budget considerations. Agencies should plan to share test time at the service provider's back-up facility ("hot site").

2. Objectives. Clearly state the purposes for conducting tests of the recovery plan. These will include aims such as the following:

   a. A disaster recovery/business resumption plan that is complete and workable.
   b. Identifying needed revisions to disaster recovery/business resumption plan.
   c. Determine the adequacy of disaster recovery/business resumption training.
   d. Identifying needed revisions to the training program.

3. Policy/Guidelines: Set up the policies and guidelines that will apply to t esting of the recovery plan. These will cover such items as the following:

   a. Committing the agency to a minimum level of testing.
   b. Basing the frequency of plan testing on the frequency of changes in the business environment. Agencies must conduct at least one test per year.

4. The testing or validation methodology adopted by an agency will depend on:

   a. Criticality of agency business functions.
   b. Cost of executing the test plan.
   c. Budget availability.
   d. Complexity of information system and components.
   e. Reporting requirements.

5. The test report should include:

    a. Date of test.
    b. Objectives of test.
    c. Description of test.
    d. Results.
    e. Recommendations.

6. Distribution list for test reports must include:

    a. DIS/PRD.
    b. Service provider if computer services are obtained from a source external to the agency.

7. User notification.

    a. Define requirements for informing users of planned tests.
    b. Before conducting any testing that requires access to client info rmation, inform the owning department. Get permission to test using the client data.

8. Specification of tests. Formulate a test schedule. For each test, specify the level of the test, the scope or areas to test, and the frequency or target date of the test.

9. Levels of testing:

    a. Level I = Adequacy of off-site storage of files and documentation.

        The purpose of the first level is the evaluation of the adequacy of the off-site storage facility and the existing recovery procedures. Primary concentration should be on the off-site files and documentation necessary for efficient system recovery.

    b. Level II = System restoration using off-site files and documentation on the in-house computers.

        The purpose of the second level is to evaluate recovery of the ability to operate. Primary concentration should be on off-site files and documentation of the operating system, as well as management control of the recovery process.

    c. Level III = System and communications restoration using alternate proc essing facilities, off-site files and documentation.

        The purpose of the third level is to evaluate recovery capability at an alternate site with a reduced staff.

10. Develop plans for specific tests.

    a. Develop test evaluation tools.
    b. Develop forms, checklists, and debriefing strategies to check recovery plan tests.

Maintenance

Assign plan maintenance responsibility.

Establish maintenance procedures and schedules. Provide a schedule for regular, systematic review of the content of the disaster recovery/business resumption plan. Define a procedure for making appropriate changes to the plan.

Develop distribution procedures and lists.

1. Provide policies and procedures for distributing the recovery plan parts and updates.
2. The disaster recovery/business resumption plan may contain sensitive information about the agency's business, communications, and computing operations. Policy and procedures for distribution of the plan should take this into account.

NOTE: DP/90 PLUS, a product of SunGard Recovery Services, is an MS-DOS software application which provides substantial help in the development and maintenance of a disaster recovery/business resumption plan. DIS has a corporate contract for this product. Because of this special contract, DP/90 PLUS is available to any state agency at a discount. Please contact DIS Leasing & Brokering Section for order information.

Glossary of Terms